549,542

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 January 2005 (27.01.2005)

PCT

(10) International Publication Number
WO 2005/008950 A1

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number:
PCT/US2004/021846

(22) International Filing Date: 9 July 2004 (09.07.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/486,127 10 July 2003 (10.07.2003) US

(71) Applicant *(for all designated States except US)*: **RSA SECURITY, INC.** [US/US]; 174 Middlesex Turnpike, Bedford, MA 01730 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **RÖSTIN, Peter** [SE/US]; 1112 Lassen Drive, Belmont, CA 94002 (US). **NYSTRÖM, Magnus** [SE/SE]; Hälsingevägen 15, S-186 35 Vallentuna (SE). **DUANE, William, M.** [US/US]; 4 Howard Road, Westford, MA 01886 (US).

(74) Agent: **RYAN, Joseph, B.**; Ryan, Manson & Lewis, LLP, 90 Forest Avenue, Locust Valley, NY 11560 (US).

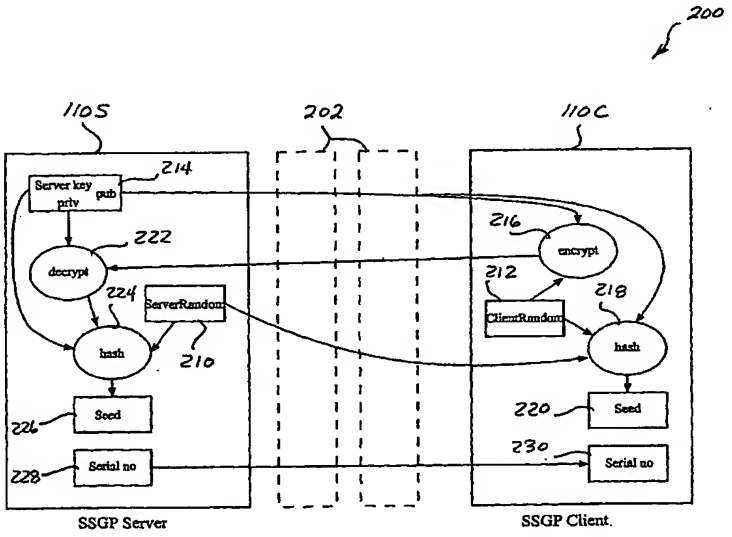
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: SECURE SEED GENERATION PROTOCOL



(57) Abstract: Techniques for secure generation of a seed for use in performing one or more cryptographic operations, utilizing a seed generation protocol carried out by a seed generation client (110c) and a seed generation server (110s). The seed generation server (110s) provides a first string to the seed generation client (110c). The seed generation client (110c) generates a second string, encrypts the second string utilizing a key (216), and sends the encrypted second string to the seed generation server (110s). The seed generation client (110c) generates the seed as a function of at leas the first string and the second string. The seed generation server (110s) decrypts the encrypted second string (222) and independently generates the seed as a function of at least the first string an the second string.

WO 2005/008950 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.